BA

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－134102
（P2003－134102A）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｇ０６Ｋ　17/00	Ｔ	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｇ０９Ｃ　1/00	６６０Ａ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｈ０４Ｌ　9/00	６２１Ａ	

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願2001－322711(P2001－322711)

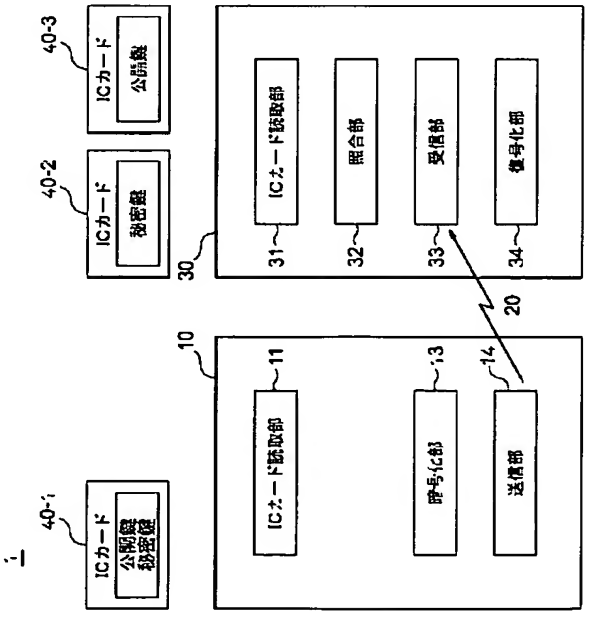
(22)出願日　平成13年10月19日(2001.10.19)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　大島　直行
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　矢野　義博
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100094053
弁理士　佐藤　隆久

最終頁に続く

(54)【発明の名称】　暗号化システム

(57)【要約】
【課題】所望のセキュリティ性、運用形態に適切に適合することができ、その結果よりセキュリティ性を高くすることのできる暗号化システムを提供する。
【解決手段】作業者がＩＣカード４０-1を送信装置１に装荷したら、ＩＣカード読み取り部１１で作業者の認証が行われ、ＩＣカードに記憶されているＲＳＡ公開鍵を用いて暗号化部１３で送信用データが公開鍵暗号化され、送信部１４よりインターネット２０を介して受信装置３０に送信される。受信側においては、作業者およびその上司が同時にＩＣカード４０-2および４０-3を受信装置３０に装荷することにより、ＩＣカード読み取り部３１で作業者および権限者の認証が行われ、照合部３２でそれら作業者および権限者の対応が照合され、対応関係が適正な場合、受信部３３が受信したデータを、復号化部３４で作業者のＩＣカード４０-2に記憶されている秘密鍵を用いて復号化する。



【特許請求の範囲】
【請求項１】所定の公開鍵暗号化方式において使用する秘密鍵が記憶された第１の情報記憶媒体と、
前記秘密鍵に対応する公開鍵が記憶された第２の情報記憶媒体と、
第１の情報記憶媒体と第２の情報記憶媒体が実質的に同時に提示されたか否かを検出する情報記憶媒体検出手段と、第１の情報記憶媒体と第２の情報記憶媒体が実質的に同時に提示された場合に前記第１の情報記憶媒体または前記第２の情報記憶媒体に記憶されている秘密鍵または公開鍵を用いて、前記暗号化方式に関わる所望の処理を行う暗号化処理手段とを有する暗号化処理装置とを有する暗号化システム。
【請求項２】前記所定の暗号化方式は公開鍵暗号方式に用いる請求項１に記載の暗号化システム。
【請求項３】前記第１の情報記憶媒体または前記第２の情報記憶媒体のいずれか一方は、前記所望の処理を行う作業者に保持され、
前記第１の情報記憶媒体または前記第２の情報記憶媒体のいずれか他方は、前記作業者の行為に責任を有する管理者に保持され、
前記管理者および前記作業者が実質的に同時に承認したときにのみ、前記所望の処理を行う請求項１または２に記載の暗号化システム。
【請求項４】所定の公開鍵暗号化方式において使用する秘密鍵および当該秘密鍵に対応する公開鍵が記憶された第３の情報記憶媒体と、
第３の情報記憶媒体が提示されたか否かを検出する情報記憶媒体検出手段と、前記第３の情報記憶媒体が提示された場合に当該第３の情報記憶媒体に記憶されている前記秘密鍵または前記公開鍵を用いて前記暗号化方式に関わる所望の処理を行う暗号化処理手段とを有する第２の暗号化処理装置と、
をさらに有し、
少なくとも前記第１の暗号化処理装置と前記第２の暗号化処理装置との間で、所望の情報を前記所定の公開鍵暗号化方式により暗号化して通信する請求項１～３のいずれかに記載の暗号化システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、たとえばインターネットを介した通信システムなどに適用して好適な、ＩＣカードを利用して情報を公開鍵暗号化するセキュリティ性の高い暗号化システムに関する。
【０００２】
【従来の技術】情報処理技術や通信技術の進展により、インターネットに代表されるような、大規模で簡単にデータを送受信することのできる環境が出現している。また一方で、業務の効率化や業務の多様化のために、そのような通信網を介した情報通信をより有効に使用して業務を遂行しようというＩＴ化への流れも急速に進んでいる。
【０００３】そのような状況の中において考慮すべき最も重要な要素の１つに、セキュリティ性を維持するという点が上げられる。たとえばインターネットを介した通信は比較的セキュリティ性が低いことから、重要なデータは暗号化して送受信されることが多い。また、その際の暗号化方式についても、種々の方式が検討され使用されている。また、通信装置を扱う作業者についても、認証処理を行った後に作業を行わせるなどの方策がとられている。
【０００４】そのようなセキュリティに対する対策がとられた従来の通信システムとしては、ＩＣカードに保有者のＩＤ番号、公開鍵および秘密鍵を記録し、送信時あるいは受信時、あるいは暗号化時あるいは復号化時に、このＩＣカードを用いて作業者の認証を行い、認証された場合にカードに記憶されているいずれかの鍵を選択して暗号化あるいは復号化を行う、というようなシステムがある。
【０００５】
【発明が解決しようとする課題】ところで、たとえば個人がＲＳＡ暗号鍵を使った暗号化あるいは復号化を行う場合には、そのような従来のシステムであっても大きな問題は無いと思われるが、会社間にて使用する場合、その元ファイルのセキュリティ性の度合いにより、復号化を行う作業者にもみられたくないというような場合がある。すなわち、特定の権限を有する権限者あるいは管理者に直接通信を行いたい場合や、少なくともそのような権限者あるいは管理者の厳密な管理の下での作業を期待する場合などである。
【０００６】一方で、そのような場合であっても、会社間の関係や規模の相違などにより、送信側においてはそのような複雑な認証を必要とせず、１人の作業者に処理を任せて問題ない場合もある。そのような場合には、送信側は一人の権限で作業が可能で、受信側は複数の者のチェックにより作業を進めるというような、表面的にはセキュリティ性に差があるようなシステムが要求される場合もある。しかしながらこれまでは、そのような要求されたセキュリティ状態、また運用形態に適切に適応できるようなシステムが存在しなかった。その結果、最もセキュリティ性の甘い部分に合ったシステムを選択するしかできず、結果的にセキュリティ性の悪いシステムとしてしまう場合があった。
【０００７】したがって本発明の目的は、所望のセキュリティ性、運用形態に適切に適合することができ、その結果よりセキュリティ性を高くすることのできる暗号化システムを提供することにある。
【０００８】
【課題を解決するための手段】前記課題を解決するために、本発明に係る暗号化システムは、所定の公開鍵暗号

化方式において使用する秘密鍵が記憶された第１の情報記憶媒体と、前記秘密鍵に対応する公開鍵が記憶された第２の情報記憶媒体と、第１の情報記憶媒体と第２の情報記憶媒体が実質的に同時に提示されたか否かを検出する情報記憶媒体検出手段と、第１の情報記憶媒体と第２の情報記憶媒体が実質的に同時に提示された場合に前記第１の情報記憶媒体または前記第２の情報記憶媒体に記憶されている秘密鍵または公開鍵を用いて、前記前記暗号化方式に関わる所望の処理を行う暗号化処理手段とを有する暗号化処理装置とを有する。

【０００９】前記所定の暗号化方式は公開鍵暗号方式である。好適には、前記第１の情報記憶媒体または前記第２の情報記憶媒体のいずれか一方は、前記所望の処理を行う作業者に保持され、前記第１の情報記憶媒体または前記第２の情報記憶媒体のいずれか他方は、前記作業者の行為に責任を有する管理者に保持され、前記管理者および前記作業者が実質的に同時に承認したときにのみ、前記所望の処理を行う。

【００１０】また好適には、所定の公開鍵暗号化方式において使用する秘密鍵および当該秘密鍵に対応する公開鍵が記憶された第３の情報記憶媒体と、第３の情報記憶媒体が提示されたか否かを検出する情報記憶媒体検出手段と、前記第３の情報記憶媒体が提示された場合に当該第３の情報記憶媒体に記憶されている前記秘密鍵または前記公開鍵を用いて前記暗号化方式に関わる所望の処理を行う暗号化処理手段とを有する第２の暗号化処理装置とをさらに有し、少なくとも前記第１の暗号化処理装置と前記第２の暗号化処理装置との間で、所望の情報を前記所定の公開鍵暗号化方式により暗号化して通信する。

【００１１】

【発明の実施の形態】本発明の一実施の形態を図１～図３を参照して説明する。本実施の形態においては、所望のデータファイルをインターネットを介して伝送する送信装置および受信装置を有する通信システムを例示して、本発明を説明する。

【００１２】まず、本実施の形態の通信システム１の概略の構成および動作について説明する。図１は、本発明の一実施の形態の通信システム１の全体の概略構成を示すブロック図である。通信システム１は、送信装置１０および受信装置３０がインターネット２０を介して接続された構成である。

【００１３】送信装置１０は、所望のデータを暗号化して、インターネット２０を介してたとえば受信装置３０に送信する。送信装置１０においては、通信作業者が、保持するＩＣカード４０-1を装荷することにより、そのＩＣカード４０-1に記憶されている公開鍵暗号化方式の公開鍵または秘密鍵を用いて、暗号化およびデータ送信の処理が行われる。なお送信装置１０は、通信機能およびＩＣカードとのインターフェイス機能を有する、パーソナルコンピュータなどにより構成される。

【００１４】受信装置３０は、インターネット２０を介してたとえば送信装置１０より送信された暗号化されたデータを受信し復号する。受信装置３０は、通信作業者が保持するＩＣカード４０-2と、たとえばその通信作業者の上司などの特定の権限者が保持するＩＣカード４０-3とが実質的に同時に受信装置３０に装荷されることにより、そのようなデータの受信および復号化の処理が可能となる。

【００１５】通信作業者が保持するＩＣカード４０-2には、送信側の通信作業者が保持するＩＣカード４０-1に記憶されている公開鍵に対応する公開鍵暗号化方式の秘密鍵が記憶されており、権限者の保持するＩＣカード４０-3には、その秘密鍵に対応する公開鍵が記憶されている。また、通信作業者および権限者が保持する各ＩＣカード４０-2および４０-3には、それらの対応が認識できるように設定されたＩＤ番号が記憶されている。したがって、まず、これらＩＣカード４０-2およびＩＣカード４０-3に記憶されているＩＤ番号が照合されることにより、通信作業者および権限者が各々適切な作業者および権限者であるか否か、また、それら適切な作業者および権限者が実質的に同時に作業に関わっているか否かが判定される。そして、それらが全て適正であった場合に、通信作業者の保持するＩＣカード４０-2に記憶されている秘密鍵を用いて、受信したデータの復号化が行われる。

【００１６】なお、実質的に同時に装荷されるとは、複数のＩＣカードインターフェイスを介してこれら２枚のＩＣカードが同時に装荷されること、あるいは、たとえば１つのＩＣカードインターフェイスを介してこれら２枚のＩＣカードが所定の短時間の間に順次連続的に装荷されることを示す。また、受信装置２０は、通信機能およびＩＣカードとのインターフェイス機能を有する、パーソナルコンピュータなどにより構成される。

【００１７】このような構成の通信システム１においては、送信側において、適切な作業者である通信作業者がＩＣカード４０-1を送信装置１０に装荷し、送信装置１０上で所望のデータを暗号化しインターネット２０を介して送信する。受信側においては、ＩＣカード４０-2を保持する通信作業者およびＩＣカード４０-3を保持する権限者が各々ＩＣカード４０-2および４０-3を受信装置３０に装荷し、同時に作業に関わった場合に、その受信したデータの復号化が可能となり、適切にデータの受信を行うことができる。

【００１８】次に、このような通信システム１のより詳細な構成および動作について図２および図３を参照して説明する。図２は、通信システム１のより詳細な構成を示すブロック図である。

【００１９】送信装置１０は、ＩＣカード読み取り部１１、暗号化部１３および送信部１４を有する。なお、ＩＣカード４０-1には、公開鍵暗号化方式の公開鍵および

そのＩＣカードの保持者を特定するＩＤ番号が記憶されている。ＩＣカード読み取り部１１は、作業者により装荷されたＩＣカード４０-1よりＩＤ番号を読み込み、その作業者が送信装置１０を介してデータの送信を行うのに適正な作業者であるか否かを検出する。そして、適正な作業者であった場合には、さらにＩＣカード４０-1よりカードに記憶されているＲＳＡ公開鍵を読み込み、暗号化部１３に出力する。

【００２０】暗号化部１３は、ＩＣカード読み取り部１１より入力される公開鍵に基づいて、作業者が指定する所望のデータを暗号化し、送信部１４に出力する。送信部１４は、暗号化部１３より入力された暗号化されたデータを、インターネット２０を介して受信装置３０に送信する。

【００２１】受信装置３０は、ＩＣカード読み取り部３１、照合部３２、受信部３３および復号化部３４を有する。なお、ＩＣカード４０-2には、公開鍵暗号化方式の秘密鍵およびそのＩＣカードの保持者を特定するＩＤ番号が、また、ＩＣカード４０-3には、公開鍵暗号化方式の公開鍵およびそのＩＣカードの保持者を特定するＩＤ番号が、各々記憶されている。

【００２２】ＩＣカード読み取り部３１は、通信作業者が装荷したＩＣカード４０-2およびその通信作業者の上司などの所定の権限者が装荷したＩＣカード４０-3より各々ＩＤ番号を読み出し、それら作業者および権限者が各々適正な作業者および権限者であるか否かを各々判定する。そして、作業者および権限者が各々適正な作業者および権限者であった場合には、読み出した各ＩＤ番号を照合部３２に出力するとともに、さらに、通信作業者が装荷したＩＣカード４０-2より秘密鍵を読み出し、復号化部３４に出力する。

【００２３】照合部３２は、ＩＣカード読み取り部３２より入力される、通信作業者および権限者の各々が装荷したＩＣカード４０-2および４０-3より読み出されたＩＤ番号を照合し、それら作業者および権限者が対応した作業者および権限者であるか否かを判定する。そして、その判定結果を復号化部３４に出力する。

【００２４】受信部３３は、インターネット２０を介して送信装置１０より送信される暗号化されたデータを受信し、復号化部３４に出力する。

【００２５】復号化部３４は、照合部３２より作業者および権限者が対応した適正な作業者および権限者であるとの判定結果が入力された場合に、受信部３３より入力される暗号化された受信データを、ＩＣカード読み取り部３１より入力される秘密鍵を用いて復号化する。

【００２６】このような構成の通信システム１においては、図３に示すように、まず、送信側において、作業者がＩＣカード４０-1を送信装置１に装荷することにより、ＩＣカード読み取り部１１において作業者の認証が行われ、作業者が適正であれば、そのＩＣカード４０-1に記憶されている公開鍵を用いて、暗号化部１３において所望の送信用データが公開鍵暗号化される。そして、公開鍵暗号化されたデータは、送信部１４よりインターネット２０を介して受信装置３０に送信される。

【００２７】受信側においては、作業者およびその上司たる権限者が同時に各ＩＣカード４０-2および４０-3を受信装置３０に装荷することにより、ＩＣカード読み取り部３１において、作業者および権限者の認証が行われる。そしてさらに、照合部３２において、それら作業者および権限者が適正に対応した作業者および権限者であるか否かが照合される。そして、作業者および権限者の各々、および、それらの対応関係が適正であった場合に、受信部３３が受信した暗号化されたデータを、復号化部３４において、作業者のＩＣカード４０-2に記憶されている秘密鍵を用いて復号化する。

【００２８】このように、本実施の形態の通信システム１においては、受信したデータを復号化する際には、作業者のＩＣカードとともに管理者の保有するＩＣカードが必要となる。したがって、作業者が単独で復号化を行うこと、すなわちデータを得ることができなくなり、よりセキュリティ性の高い通信システムが構築される。

【００２９】なお、本発明は本実施の形態に限られるものではなく、任意好適な種々の改変が可能である。たとえば、本実施の形態においては、受信側において、作業者が秘密鍵の記憶されたＩＣカード、管理者が公開鍵の記憶されたＩＣカードを保持するようにしたが、これに限られるものではない。たとえば、管理者が秘密鍵の記憶されたＩＣカードを保持し、作業者が公開鍵の記憶されたＩＣカードを保持するようにしてもよい。また、職制上の上下関係に関わらず、同等な二人の作業者がこれらのカードを保持するようにしてもよい。

【００３０】また、本実施の形態においては、送信装置および受信装置を区別して説明を行ったが、通常これらは１の通信装置として構成されるべきものであり、実際にはそのような構成でよい。このような場合、受信装置３０においては、作業者および管理者が各々保持する２枚のＩＣカードが同時に装置に装荷された場合にデータの暗号化および送信が可能となる。そしてその際には２枚のＩＣカードのいずれか一方に記憶されている公開鍵が使用されて、暗号化が行われる。また、このような場合、送信装置１０においては、作業者が保持する１枚のＩＣカードに公開鍵および秘密鍵の両方が記憶されているようにし、その秘密鍵を用いて受信装置３０より送信されたデータを復号化するようにするのが好適である。本発明の主旨は、少なくとも一方の通信側において、複数の作業者または管理者により承認された状態で暗号化および復号化を行うことにある。したがって、通信形態、鍵の保有形態などの前述した程度の変形は本発明の範囲内である。

【００３１】また、本実施の形態においては、各ＩＣカ

ードの保有者の認証は、ＩＣカードに記憶されているＩＤ番号に基づいて行うものとした。しかしながら、ＩＣカードに記憶されている秘密鍵または公開鍵などを用いてこれを行うようにしてもよい。

【００３２】

【発明の効果】このように、本発明によれば、所望のセキュリティ性、運用形態に適切に適合することができ、その結果よりセキュリティ性を高くすることのできる暗号化システムを提供することができる。

【図面の簡単な説明】

【図１】図１は、本発明の一実施の形態の通信システムの概略構成を示す図である。

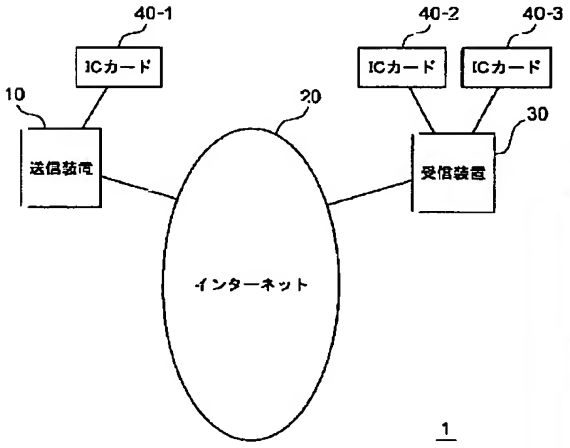
【図２】図２は、図１に示した通信システムのより詳細な構成を示す図である。

【図３】図３は、本実施の形態の通信システムの動作を模式的に示す図である。

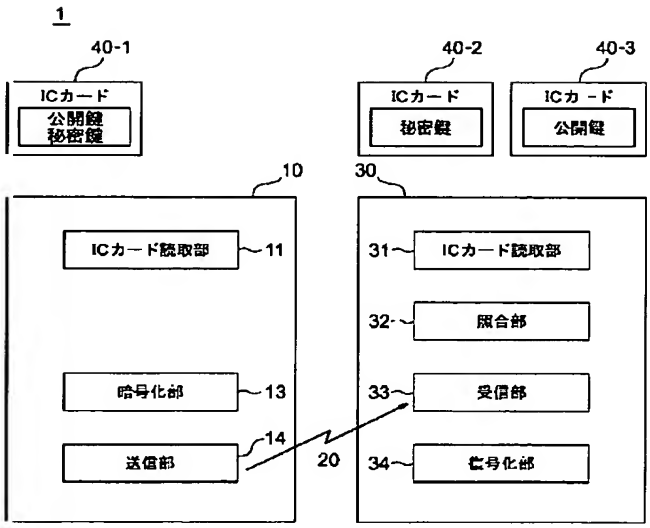
【符号の説明】

１…通信システム
１０…送信装置
１１…ＩＣカード読取部
１３…暗号化部
１４…送信部
２０…インターネット
３０…受信装置
３１…ＩＣカード読取部
３２…照合部
３３…受信部
３４…復号化部
４０…ＩＣカード

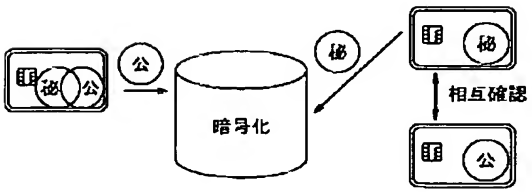
【図１】



【図２】



【図３】



フロントページの続き

Ｆターム(参考) 5B058 CA27 KA02 KA04 KA31 KA33
KA35
5J104 AA16 EA22 JA28 NA02 NA35
NA36 NA37 PA07

Japanese Kokai Patent Application No. P2003-134102A

Job No.: 228-117009
Ref.: Japanese patent no. 2003-134102/PU030342 US/PPK(Fideliz)/Order No. 7779
Translated from Japanese by the McElroy Translation Company
800-531-9977 customerservice@mcelroytranslation.com

JAPANESE PATENT OFFICE
PATENT JOURNAL(A)
KOKAI PATENT APPLICATION NO. 2003-134102A

Int. Cl.[7]:	H 04 L 9/10 G 06 K 17/00 G 09 C 1/00
Filing No.:	P2001-322711
Filing Date:	October 19, 2001
Publication Date:	May 9, 2003
No. of Claims:	4 (Total of 5 pages; OL)
Examination Request:	Not filed

ENCRYPTION SYSTEM

Inventors: Naoyuki Oshima
Dainippon Printing Co., Ltd.
1-1-1 Ichigayakaga-cho,
Shinjuku-ku, Tokyo

Yoshihiro Yano
Dainippon Printing Co., Ltd.
1-1-1 Ichigayakaga-cho,
Shinjuku-ku, Tokyo

Applicant: 000002897
Dainippon Printing Co., Ltd.
1-1-1 Ichigayakaga-cho,
Shinjuku-ku, Tokyo

Agent: 1000940553
Takahisa Sato, patent attorney

[There are no amendments to this patent.]

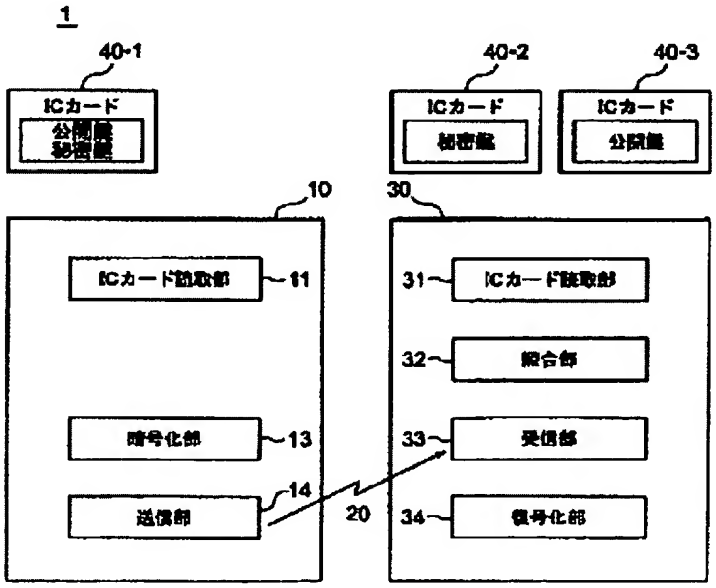
Abstract

Problem

To provide an encryption system which can be appropriately adapted to the desired security level and the application, so that it is possible to maintain the higher security level.

Means to solve

When an operator inserts IC card (40-1) into transmitter (1), IC card reader (11) verifies the identity of the operator, encryption part (13) uses an RSA public key stored in the IC card to encrypt data for transmission with the public key, and transmitting part (14) transmits the encrypted data to receiver (30) via the Internet (20). On the receiving side, an operator and his/her supervisor simultaneously insert IC cards (40-2) and (40-3) in receiver (30), and IC card reader (31) thereby authenticates the operator and the authorized person. Collator (32) collates the correspondence between the operator and the authorized person. If the correspondence relation is appropriate, the data received by receiving part (33) are decrypted by means of the confidential key stored in IC card (40-2) of the operator by decryption part (34).



Key:
11 IC card reader
13 Encryption part
14 Transmitting part
31 IC card reader
32 Collator
33 Receiving part

34 Decryption part
40-1 IC card
Public key
Confidential key
40-2 IC card
Confidential key
40-3 IC card
Public key

Claims

1. An encryption system characterized in that it comprises of the following parts:

a first information storage medium in which a confidential key is stored for use in the prescribed public key encryption system,

a second information storage medium in which the public key corresponding to said confidential key is stored,

and an encryption processor that includes an information storage medium detection means that detects whether the first information storage medium and the second information storage medium are presented more or less simultaneously, and an encryption processing means that performs the prescribed processing pertaining to said encryption system by using the confidential key or public key stored in said first information storage medium or said second information storage medium if said first information storage medium and said second information storage medium are presented more or less simultaneously.

2. The encryption system described in Claim 1, characterized in that said prescribed encryption system is used in the public key encryption system.

3. The encryption system described in Claim 1 or 2, characterized in that:

the operator who performs said desired processing holds either said first information storage medium or said second information storage medium,

of said first information storage medium and second information storage medium, the one that is not held by the operator is held by the supervisor who is responsible for the actions of said operator,

and said desired operation is performed only if said supervisor and said operator are acknowledged at effectively the same time.

4. The encryption system described in any of Claims 1-3, characterized in that it also includes

a third information storage medium in which the confidential key for use in the prescribed public key encryption system and the public key corresponding to said confidential key are stored,

and a second encryption processor that includes an information storage medium detection means that detects whether said third information storage medium is presented, and an encryption processing means that performs the desired processing pertaining to said encryption system using said confidential key or said public key stored in said third information storage medium if said third information storage medium is presented;

wherein the desired information is encrypted by said prescribed public key encryption system and is communicated between at least said first encryption processor and said second encryption processor.

Detailed explanation of the invention

[0001]

Technical field of the invention

The present invention pertains to an encryption system with a high security level that can be preferably used in a communication system, etc., via, the Internet, e.g., and uses an IC card to encrypt the information with a public key.

[0002]

Prior art

With the development of information processing and communications technology, there appears to be an environment in which data transmission/reception can be easily performed on a large scale. On the other hand, in order to improve the efficiency of conducting diverse transactions, there is a trend toward quickly developing an IT method of conducting transactions so that information can be communicated more efficiently via communications networks.

[0003]

One of the most important factors that should be taken into consideration in this context pertains to maintaining the security levels. For example, communication via the Internet characterized by a relatively low security level, so that important data should be encrypted for transmission/reception. Various encryption systems have been studied and adopted for this purpose. Also, an operator that handles a communication device can initiate operations after his/her identity has been verified.

[0004]

A communication system that adopts the aforementioned security measures of the prior art operates as follows: the ID No., public key and confidential key of the IC card owner are recorded; during transmission/reception, or during encryption or decryption, the identity of the

operator using said IC card is verified. After verification, a certain key stored in the card is selected to encrypt or decrypt data.

[0005]

Problems to be solved by the invention

However, if someone uses an RSA encryption key to encrypt or decrypt data, it is thought for example, that the aforementioned conventional system will pose no major problems. However, when it is used between companies, depending on the security level of the original file, the operator may not be allowed to read the file. That is, if direct communication is to be performed with an authorized person or his/her supervisor with assigned prescribed rights, the operation should at least be able to be performed under the strict supervision by said authorized person or his/her supervisor.

[0006]

On the other hand, even in such cases, depending on the relationship between the companies and the difference in scale, there may be no need for complicated verification on the transmitting side, and a single operator may be able to perform the required operations without any problems. In such cases, the operation can be performed by a single person on the transmitting side and by plural persons on the receiving side who conduct verification processes. The difference in security levels between the two sides may be apparent. But no appropriate systems that can accommodate the requested security level or application exist. As a result, it is only possible to select a system that can be adapted to the more easily handled security. Consequently, the security level of the system may become too low.

[0007]

Consequently, the purpose of the present invention is to provide an encryption system that can be appropriately adapted to the desired security level and the given application, so that the higher security level can be maintained.

[0008]

Means to solve the problems

In order to solve the aforementioned problem, the present invention provides an encryption system characterized in that it comprises the following: a first information storage medium in which a confidential key for use in the prescribed public key encryption system is stored, a second information storage medium in which the public key corresponding to said confidential key is stored, and an encryption processor that includes an information storage

medium detection means that detects whether the first information storage medium and the second information storage medium are presented more or less simultaneously, and an encryption processing means, which performs the prescribed processing pertaining to said encryption system by using the confidential key or public key stored in said first information storage medium or said second information storage medium if said first information storage medium and said second information storage medium are presented more or less simultaneously.

[0009]

Said prescribed encryption system is a public key encryption system. The following scheme is preferred: the operator who performs said desired processing holds either said first information storage medium or said second information storage medium; of said first information storage medium and second information storage medium, the one that is not held by the operator is held by the supervisor who is responsible for the actions of said operator, and said desired operation is performed only when said supervisor and said operator are acknowledged at effectively the same time.

[0010]

Also, the following scheme is preferred: the system also comprises a third information storage medium, in which the confidential key for use in the prescribed public key encryption system and the public key corresponding to said confidential key are stored, and a second encryption processor that includes an information storage medium detection means, which detects whether said third information storage medium is presented, and an encryption processing means, which performs the desired processing pertaining to said encryption system using said confidential key or said public key stored in said third information storage medium if said third information storage medium is presented; wherein the desired information is encrypted by said prescribed public key encryption system and is communicated between at least said first encryption processor and said second encryption processor.

[0011]

Embodiment of the invention

In the following, an explanation will be given regarding an embodiment of the present invention with reference to Figures 1-3. In this embodiment, the present invention is explained with reference to a communication system that includes a transmitter and a receiver that perform transmission via the Internet.

[0012]

First, the schematic constitution and operation of communication system (1) of the present embodiment will be explained. Figure 1 is a block diagram schematically illustrating the overall communication system (1) in an embodiment of the present invention. Said communication system (1) includes transmitter (10) and receiver (30) connected via the Internet (20).

[0013]

Said transmitter (10) encrypts the desired data, and transmits the encrypted data via the Internet (20) to receiver (30). In transmitter (10), the encryption and processing of data for transmission is performed when the operator inserts his/her IC card (40-1) by using the public key or confidential key in the public key encryption system stored in said IC card (40-1). Also, transmitter (10) is a personal computer etc., that has a communication function and interface function with the IC card.

[0014]

Said receiver (30) receives and decodes the encrypted data transmitted from transmitter (10) via the Internet (20). For receiver (30), when IC card (40-2) held by the communication operator and IC card (40-3) held by the supervisor or another prescribed authorized person are inserted in receiver (30) at effectively the same time, it is possible for data to be received and decrypted.

[0015]

The confidential key of the public key encryption system corresponding to the public key stored in IC card (40-1) held by the communication operator on the transmission side is stored in IC card (40-2) held by the communication operator, and the public key corresponding to said confidential key is stored in IC card (40-3) held by the authorized person. Also, an ID No. is stored in each of said IC card (40-2) held by the communication operator and IC card (40-3) held by the authorized person that is used to recognize said correspondence relation. Consequently, first by checking the ID Nos. stored in IC card (40-2) and IC card (40-3), it is determined whether the communication operator and the authorized person are the legitimate operator and authorized person, respectively, and whether the legitimate operator and authorized person are performing their operations at effectively the same time. If so, the confidential key stored in IC card (40-2) held by the communication operator is used to decrypt the received data.

[0016]

If both IC cards are inserted at effectively the same time, it is made known that said two IC cards were inserted simultaneously via plural IC card interfaces, or that said two IC cards were successively inserted within a prescribed short time interval via a single IC card interface. Also, the Internet (20) is accessed on a personal computer that has a communication function and interface function with the IC card.

[0017]

In communication system (1) with said constitution, on the transmitting side, the verified communication operator inserts IC card (40-1) in transmitter (10), the desired data are encrypted on transmitter (10) and are transmitted via the Internet (20). On the receiving side, the communication operator who holds IC card (40-2) and the authorized person who holds IC card (40-3) insert said IC cards (40-2) and (40-3) in receiver (30), and, since the operation is performed simultaneously, the received data can be decrypted, and appropriate data reception can be performed.

[0018]

In the following, an explanation will be given regarding the detailed constitution and operation of communication system (1) with reference to Figures 2 and 3. Figure 2 is a block diagram illustrating the detailed constitution of communication system (1).

[0019]

Said transmitter (10) includes IC card reader (11), encryption part (13) and transmitting part (14). Said IC card (40-1) stores the public key of the public key encryption system and the ID No. for identifying the holder of the IC card. Said IC card reader (11) reads the ID No. from IC card (40-1) inserted by the operator, and it detects whether the operator is authorized to transmit data via transmitter (10). If so, the RSA public key stored in the card is read from IC card (40-1) and output to encryption part (13).

[0020]

Said encryption part (13) encrypts the desired data assigned by the operator on the basis of the public key input by IC card reader (11), and it outputs the result to transmitting part (14). Said transmitting part (14) transmits the encrypted data input from encryption part (13) via the Internet (20) to receiver (30).

[0021]

Said receiver (30) includes IC card reader (31), collator (32), receiving part (33) and decryption part (34). Said IC card (40-2) stores the confidential key of the public key encryption system and the ID No. specifying the holder of the IC card. Said IC card (40-3) stores the public key of the public key encryption system and the ID No. specifying the holder of the IC card.

[0022]

Said IC card reader (31) reads the ID Nos. from IC card (40-2) inserted by the communication operator and IC card (40-3) inserted by the supervisor of the communication operator or an authorized person, and it checks whether the operator and the authorized person are the legitimate operator and authorized person, respectively. If so, the read ID Nos. are output to collator (32), and the confidential key is read from IC card (40-2) inserted by the communication operator and output to decryption part (34).

[0023]

Said collator (32) checks the ID Nos. read from inserted IC card (40-2) and IC card (40-3) inserted by the communication operator and the authorized person, respectively, input from IC card reader (32) [sic; (31)], and collates the correspondence between the operator and the authorized person. The collation result is output to decryption part (34).

[0024]

Said receiving part (33) receives the encrypted data transmitted from transmitter (10) via the Internet (20), and outputs the data to decryption part (34).

[0025]

When the collation result input from collator (32) verifies the correspondence between the operator and the authorized person, decryption part (34) decrypts the encrypted data input received by receiving part (33) by means of the confidential key input by IC card reader (31).

[0026]

In communication system (1) with said constitution, as shown in Figure 3, first, when the operator inserts IC card (40-1) in communication system (1), IC card reader (11) verifies the operator. If the operator is verified, the public key stored in said IC card (40-1) is used to encrypt the desired data for transmission in encryption part (13) with the public key. Then, the public key encrypted data are transmitted by transmitting part (14) to receiver (30) via the Internet (20).

[0027]

On the receiving side, the operator and his/her supervisor or an authorized person simultaneously insert IC cards (40-2) and (40-3), respectively, in receiver (30), in IC card reader (31), and the operator and the authorized person are verified. In addition, collator (32) collates the correspondence between the operator and the authorized person. Once the operator and the authorized person have both been verified, and their correspondence relation is appropriate, the encrypted data received by receiving part (33) are decrypted with the confidential key stored in IC card (40-2) of the operator in decryption part (34).

[0028]

As explained above, in communication system (1) of the present embodiment, when the received data are decoded, it is necessary to have both the IC card of the supervisor and the IC card of the operator. Consequently, if the operator attempts to decrypt by himself or herself, it will be impossible to obtain the data, so a communication system with a high security level can be constructed.

[0029]

The present invention is not limited to the aforementioned embodiment, and any appropriate modification can be performed. For example, in the present embodiment, on the receiving side, the confidential key is stored in the IC card of the operator and the public key stored in the IC card of the supervisor. However, the present invention is not limited to this scheme. For example, a scheme in which the supervisor holds the IC card with the stored confidential key, and the operator holds the IC card with the stored public key. Also, said cards may be held by two equal-level employees regardless of their relative status.

[0030]

In the explanation of the embodiment above, a discrete transmitter and receiver were treated separately. However, they are usually integrated into a single communication device (1), and such a constitution may also be used in practice. In such cases, with receiver (30), it is possible to encrypt and transmit data when the two IC cards held by the operator and the supervisor, respectively, are inserted simultaneously. In this case, the public key stored in either of said two IC cards is used for encryption. In such a case, in transmitter (10), both the public key and the confidential key are stored in a single IC card held by the operator, and the confidential key is used to decode the data transmitted from receiver (30). The essence of the present invention is that on at least one communication side, the encryption and decoding are performed with the acknowledgement of plural operators or supervisors. Consequently,

modification of the configuration, how the keys are held, etc. is within the scope of the present invention.

[0031]

In this embodiment, the verification of the holders of the IC cards is performed on the basis of the ID Nos. stored in the IC cards. However, a scheme in which the confidential key or public key is stored in the IC card can also be used.

[0032]

Effects of the invention

As explained above, the encryption system of the present invention can be used to adapt appropriately to the desired security level and the given application. As a result, it is possible to maintain the security level with the encryption system of the present invention.

Brief description of the figures

Figure 1 is a diagram illustrating the schematic constitution of the communication system in an embodiment of the present invention.

Figure 2 is a diagram illustrating the detailed constitution of the communication system shown in Figure 1.

Figure 3 is a schematic diagram illustrating the operation of the communication system in the present embodiment.

Explanation of symbols

1 Communication system
10 Transmitter
11 IC card reader
13 Encryption part
14 Transmitting part
20 The Internet
30 Receiver
31 IC card reader
32 Collator
33 Receiving part
34 Decryption part
40 IC card

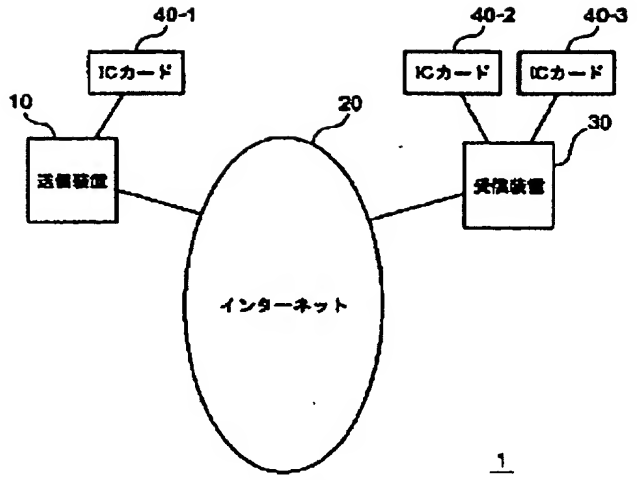


Figure 1

Key: 10 Transmitter
20 The Internet
30 Receiver
40-1, 40-2, 40-3 IC card

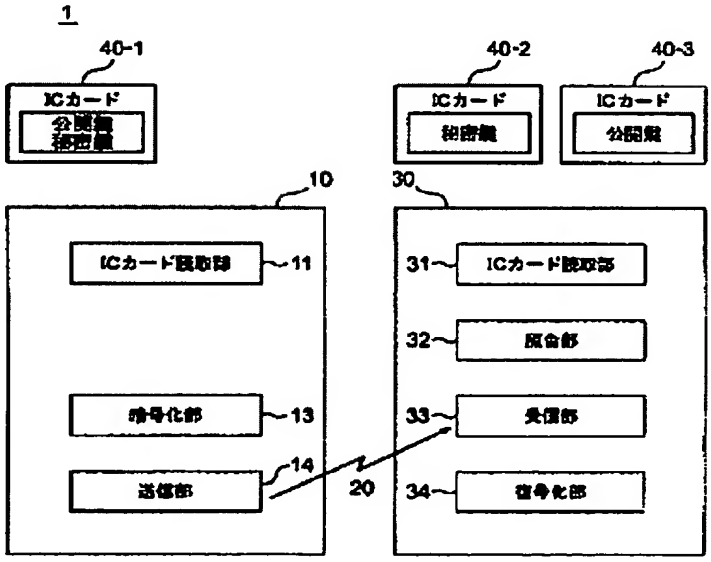


Figure 2

Key: 11 IC card reader
13 Encryption part
14 Transmitting part
31 IC card reader

32 Collator
33 Receiving part
34 Decryption part
40-1 IC card
Public key
Confidential key
40-2 IC card
Confidential key
40-3 IC card
Public key

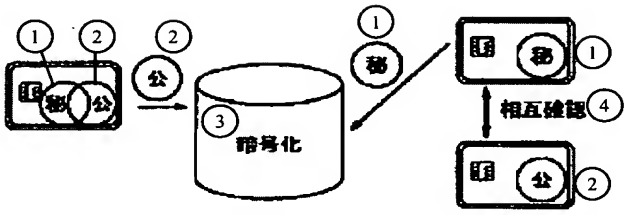


Figure 3

Key: 1 Confidential
2 Public
3 Encryption
4 Mutual verification